

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Nº 13-CR-607 (JFB)

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

★ **AUG 28 2015** ★

LONG ISLAND OFFICE

UNITED STATES OF AMERICA,

VERSUS

PHILLIP KENNER,

Defendant.

MEMORANDUM AND ORDER

August 28, 2015

JOSEPH F. BIANCO, District Judge:

On October 29, 2013, a grand jury returned an indictment charging Phillip Kenner ("Kenner" or "defendant") with conspiring to commit wire fraud, conspiring to launder money, and eight substantive counts of wire fraud. The defendant was then charged in a second superseding indictment, dated April 22, 2015.¹ The allegations in the indictment center on Kenner's role as an investment advisor to current and former National Hockey League players, among other clients. The government contends that Kenner was involved in three alleged schemes to defraud investors: (1) sham investments in land

development projects; (2) diversions from a litigation fund relating to the real estate investments, and (3) diversions of investments in a company called Eufora.

On January 26, 2015, the defendant moved to suppress evidence seized from his laptop computer and iPhone, arguing that the government has unreasonably retained possession of his devices in violation of his Fourth Amendment rights. The government opposed the motion to suppress on February 24, 2015. The Court held oral argument on the motion on March 13, 2015.²

For the reasons set forth herein, and the reasons set forth on the record on March 13, 2015, the motion to suppress is denied. In short, the Court concludes that the government's retention of the defendant's computer (and an imaged copy of his hard

¹ The second superseding indictment charges Kenner with conspiring to commit wire fraud, conspiring to launder money, and seven substantive counts of wire fraud. The original and superseding indictments also contain charges against Tommy Constantine as a co-defendant and alleged co-conspirator. The charges against Constantine are not relevant to the instant motion.

² At the conclusion of the oral argument, the Court denied the motion on the record, noting that this written opinion would follow.

drive) was reasonable, because the volume of documents on the computer required a prolonged review of the hard drive before the government could determine which files were within the scope of the warrant, and which files were not privileged. The Court's ruling is limited to the circumstances of this case, which compelled the government to review the defendant's hard drive in two stages. First, prosecutors who were screened off from the trial team searched through the files to identify documents that might contain privileged communications with attorneys. Once that process was complete—which only occurred a matter of weeks before the trial began—the trial team began determining which files were within the scope of the warrant by running various term searches and culling the responsive files. Contrary to the defendant's position, the government did not unreasonably delay in searching the imaged copy of plaintiff's hard drive, and thus the government's retention of the defendant's computer until the date of his trial was not unreasonable. With respect to the defendant's iPhone, the Court concludes that authentication concerns arising from audio recordings contained on the device rendered necessary (and, thus, reasonable) the continued retention of the iPhone as evidence. Accordingly, the defendant is not entitled to suppression of the evidence seized from his laptop and iPhone pursuant to the search warrant.

I. BACKGROUND

The following facts, which are not in dispute, are drawn from the defendant's motion.

On November 13, 2013, Magistrate Judge Bridget S. Bade of the District of Arizona signed a search warrant authorizing the government to search Kenner's home and seize, among other items, any "computers or storage media" that contained

records or information used as part of a wire fraud and money laundering conspiracy. (Warrant, ECF No. 154-4.) The warrant made clear that "[t]he information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence, and instrumentalities" of the crimes for which the warrant was sought. (*Id.* at 5.) The warrant authorized seizure of the laptop for off-site review, because it would have been impracticable for the government to review the computer and extract the relevant files at the time of the search warrant execution. (Affidavit of Agent Joshua Wayne in Support of Warrant Application, ECF No. 154-4 ¶¶ 39-42.)

On November 13, 2013, the government executed the warrant at Kenner's home in Scottsdale, Arizona. Among other items, the government seized the defendant's iPhone and his laptop computer. In addition to retaining the original computer, the government also duplicated the defendant's hard drive, creating what is alternately termed a "mirror image" or "forensic image" of the hard drive. The purpose of creating the mirror image was to preserve the condition of the original hard drive and the metadata contained therein, so that the government could review the files on the mirror image without disturbing the original data on the laptop.

The government was not able to immediately review the mirror image for files responsive to the warrant, because the defendant's hard drive contained many documents that were likely subject to the attorney-client privilege.³ The warrant itself

³ The government was investigating whether the defendant diverted funds that investors had contributed to a legal fund, and accordingly the government had reason to believe that defendant's computer was likely to contain communications with

provided a procedure for resolving this issue, and directed that a designated Assistant United States Attorney (AUSA) and agent be assigned to review the hard drive for information that might be privileged. The government has referred to the reviewers as the “taint team,” because they were screened off from the trial team. As the warrant required, the “taint team” knew nothing about the case, and was not involved in the investigation or the prosecution. The reviewing team was responsible for identifying documents that might be privileged, notifying the defense, and resolving any privilege issues. The trial team was not permitted to review the hard drive until that process was completed.

The government disclosed a copy of the mirror image to the defense on March 24, 2014, and the reviewing team began the lengthy process of identifying documents that might be privileged. On November 3, 2014, the government’s privilege review concluded, and the prosecutor assigned as firewall counsel contacted defense counsel to resolve any privilege issues. That process took many months, for several reasons. According to defense counsel, the documents the government identified as privileged were provided on password-protected discs, and defense counsel had some difficulty reviewing those documents. (Def. Mem. at 4.) Additionally, the review process required defense counsel to review voluminous submissions from the government, to assess their categorization of the documents, which the government had tagged as either “privileged,” “not privileged,” or “unclear.” In fact, at the time of the defendant’s motion, defense counsel and the privilege team had not yet concluded resolving all privilege issues, (Def. Mem. at

3-4), and the process continued while the present motion was briefed and argued. In particular, at the oral argument, one of the trial team AUSAs advised the Court that, as a result of this prolonged privilege-review process, the trial team had only recently obtained access to the non-privileged documents in the hard drive to search for relevant documents and that search was ongoing. (See March 13, 2015 Tr. at 55 (“[W]e’ve only recently gotten access to the non-privileged documents and for that matter the non-privileged sections of the hard drive in the original computer.”); see also *id.* at 57 (“We are methodically searching what’s in the hard drive but because of the volume and the number of individuals, the number of transactions and the date ranges, the search right now continues to go on.”).) The docket sheet further reflects that, on March 30, 2015, the AUSA assigned to the privilege review wrote a letter to defense counsel, notifying him that the privilege team intended to disclose additional non-privileged documents to the investigative team by April 8, 2015, absent any further objection from the defendant to the documents identified by the government as not privileged. (ECF No. 191.) These additional documents had initially been designated as “unclear” during the privilege review and sent to defense counsel, because it was unclear from the face of the document whether a privilege existed. (*Id.*) Thus, the docket sheet reflects that the trial team was not able to review the entire hard drive for non-privileged documents responsive to the warrant until approximately three weeks before trial began.

A jury was empaneled on April 27, 2015, and trial commenced on May 4, 2015. The jury returned its verdict on July 9, 2015, finding defendant Constantine guilty on all seven counts in which he was charged, and defendant Kenner guilty of Counts One,

his attorney and other documents relating to several civil lawsuits.

Two, Three, Four, Seven, and Nine (and not guilty on Counts Five, Six, and Eight. On consent of the parties, the forfeiture phase of the case will be conducted by the Court. The government continues to retain the iPhone, the computer, and the mirror image hard drive.

II. MOTION TO SUPPRESS EVIDENCE SEIZED FROM DEFENDANT'S LAPTOP

The defendant moves to suppress all evidence obtained from his laptop, arguing that the manner in which the government executed the warrant did not comport with the Fourth Amendment's reasonableness requirement. To be clear, the defendant does not dispute that the government lawfully seized the laptop pursuant to a search warrant, and lawfully created a mirror image of the hard drive. Moreover, the defendant does not contest that the government was entitled to conduct an off-site review of the hard drive to determine what files were responsive to the warrant. Instead, the basis of the defendant's motion is his contention that the government has unlawfully retained the original computer and the mirror image (without purging unresponsive files) for an unreasonable period of time. The government does not contest that the laptop contains documents that are beyond the scope of the warrant.

Under well-settled Second Circuit case authority, "[g]overnment agents 'flagrantly disregard' the terms of a warrant so that wholesale suppression is required only when (1) they effect a 'widespread seizure of items that were not within the scope of the warrant,' . . . and (2) do not act in good faith." *United States v. Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (quoting *United States v. Matias*, 836 F.2d 744, 748 (2d Cir. 1988)) (citations omitted). As the Second Circuit has noted, "[t]he rationale for blanket

suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search." *Liu*, 239 F.3d at 141.

The defendant's motion almost exclusively relies upon the Second Circuit's decision in *United States v. Ganas*, 755 F.3d 125 (2d Cir. 2014), which addressed a Fourth Amendment challenge to the seizure and retention of a mirror image hard drive. As the Court in *Ganas* explained, "the creation of mirror images for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be. . . . The off-site review of these mirror images, however, is still subject to the rule of reasonableness." *Id.* at 136. In *Ganas*, the government created a mirror image of the defendant's hard drive for off-site review, and completed the process of segregating responsive files thirteen months after the mirror image was created. However, the government continued to retain the hard drive after the file review had concluded. As the investigation progressed, the government began to suspect the defendant's involvement in other criminal activity. A year and a half after the file review had completed, the government sought a second warrant to search the hard drive. The Second Circuit held that suppression of all evidence seized pursuant to the second warrant was required, because the government's continued retention of the mirror image was unreasonable and violated the defendant's Fourth Amendment rights. *Ganas*, 755 F.3d at 28-31.⁴

⁴ On June 29, 2015, the Second Circuit issued a decision stating that the appeal would be reheard *en Banc*, including briefing on the following two issues: "(1) Whether the Fourth Amendment was violated when, pursuant to a warrant, the government seized and cloned three computer hard drives containing both responsive and non-responsive files, retained the

Here, it is undisputed that the government retained Kenner's computer (and a mirror image of his hard drive) for seventeen months between the initial seizure and the commencement of the trial. Although the defendant argues that *Ganias* held that a similar period of time was unreasonable, the Court is not persuaded that *Ganias* compels suppression here. As the government correctly points out, the holding in *Ganias* was expressly limited to the issues on appeal, and the Second Circuit carefully delineated the bounds of the appellate issues in the following manner:

[W]e need not address whether (1) the description of the computer files to be seized in the 2003 warrant was stated with sufficient particularity; (2) the 2003 warrant authorized the government to make a mirror image of the entire hard drive so it could search for relevant files off site; or (3) the resulting sorting process was unreasonably long. Instead, we consider a more limited question: whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations. We hold that it does not.

Id. at 28-29 (citations omitted). Given that the defendant's challenge in this case concerns the length of the sorting process, it

cloned hard drives for some two-and-a-half-years, and then searched the non-responsive files pursuant to a subsequently issued warrant; and (2) Considering all relevant factors, whether the government agents in this case acted reasonably and in good faith such that the files obtained from the cloned hard drives should not be suppressed." *United States v. Ganias*, 791 F.3d 290 (2d Cir. 2015). Oral argument is scheduled for September 30, 2015.

is clear that *Ganias* is inapposite, because the Second Circuit emphasized that its ruling did reach that issue. Instead, the limited ruling of *Ganias* was that the government may not retain a hard drive for possible use in future investigations if the hard drive contains files beyond the scope of the original warrant. Defense counsel has not argued in this case that the government has retained the hard drive for future investigative purposes, and the government has represented that it has only retained the hard drive for authentication purposes. *See United States v. Scully*, No. 14-CR-208 (ADS), 2015 U.S. Dist. LEXIS 73831, at *93 (E.D.N.Y. June 8, 2015) ("Here, the retention of documents allegedly outside the scope of the [warrants] mirrors the two and half year time-frame deemed unreasonable in *Ganias*. However, the Government states that any such emails are being retained for authentication purposes only and will not be used in future criminal investigations. Accordingly, consistent with *Ganias*, suppression is not an appropriate remedy for the alleged improper retention."). Accordingly, the Court concludes that *Ganias* does not require suppression here.

In any event, the circumstances of this case are materially distinct from those presented in *Ganias*. In *Ganias*, the government retained the hard drive over for a year and a half after the file review process was complete. In this case, the government was unable to segregate responsive files on the hard drive because of privilege issues. As a result, the investigative team could not review the hard drive until the privilege team had finished segregating privileged documents—a process which was lengthy, and further prolonged by the need to confer with defense counsel to verify the government's privilege determinations. Consequently, the substantive review of the hard drive by the trial team did not begin until shortly before trial. It bears

emphasizing that the privilege team was not in any way involved in the prosecution of this case, and the trial team gained no investigative advantage from retaining the hard drive during the privilege review stage of the process. On the contrary, the trial team was disadvantaged by the delay in reviewing the hard drive for relevant documents. The lengthy privilege review process left the trial team with only a few weeks before trial to search the hard drive for relevant material. To state the obvious, several weeks is not an unreasonably long period of time to review voluminous records on a hard drive. *See United States v. Romain*, No. 13 CR. 724 (RWS), 2014 U.S. Dist. LEXIS 166500, at *21 (S.D.N.Y. Dec. 1, 2014) (“[T]here is no defined time period in which the Government must segregate the data responsive to the warrant from the unresponsive, though some recent case law has outlines the broad contours of what is considered reasonable.”) (citing *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) (“[U]nder current law there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant Numerous cases hold that a delay of several months between the seizure of electronic evidence and the completion of the government’s review of that evidence as to whether it falls within the scope of the warrant is reasonable.”)). Although the defendant asserts that the privilege team could have simultaneously conducted a substantive review of the mirror image to segregate and purge any files that were beyond the scope of the warrant, and thereby shortened the review process, the Court disagrees. The very purpose of establishing firewall procedures for the privilege review was to ensure that the team reviewing the hard drive was not in any way involved in the prosecution of the case. Therefore, it

would have been impossible—and, more importantly, improper—for firewall counsel to determine what files might be evidence relating to the government’s case. Based upon the constraints imposed by the review process, the Court concludes that the government did not unreasonably delay in reviewing the hard drive and segregating the unresponsive files.

Finally, to the extent the defendant’s motion rests on the fact that the government retained both the defendant’s physical computer *and* the mirror image, that argument lacks merit. Rule 41 authorizes the government to create a mirror image of a seized hard drive, *see Fed. R. Crim. P. 41(e)(2)(B)*, and the defendant has not offered any authority for the proposition that the government may not both seize the original computer and make a copy of the hard drive. Additionally, the government asserts that it retained the original computer to defeat any challenge to the mirror image’s authenticity as a copy of the original hard drive. The government also asserts that purging unresponsive files from the mirror image was impracticable, because it would compromise the remaining data that was responsive to the warrant. The defendant argues that the Second Circuit was skeptical of that very same argument in *Ganias*. *See id.* at 35 (“We are not convinced that there is no other way to preserve the evidentiary chain of custody.”). However, courts have observed that “[w]hile *Ganias* expressed skepticism about the need for retaining non-responsive files for this purpose, it was willing to ‘assume’ the need existed and stated that in such an event, the retained material should not be used ‘for any other purpose’—presumably referring to the material’s use in that case as the basis for a second warrant.” *Scully*, 2015 U.S. Dist. LEXIS 73831, at *93 (quoting *In re A Warrant for All Content & Other Information Associated With the Email*

Account xxxxxx@gmail.com Maintained At Premises Controlled By Google, Inc., 33 F. Supp. 3d 386, 399 n.7 (S.D.N.Y. July 18, 2014)).

Based upon the circumstances of this case, the Court concludes that the government's concerns about authentication in this case were well founded, and merited the retention of the laptop (and the cell phone) for authentication purposes. Even after the search process was complete on the eve of trial, it was entirely unclear that authentication issues were not going to arise during the course of the trial.⁵ Moreover, the operability of the original computer was relevant to the government's case-in-chief because there was testimony that Kenner told at least one investor, several weeks before the laptop was seized, that he could not provide them with documentation of their investments because his laptop was broken. Thus, at trial, the original device itself was introduced into evidence by the government to demonstrate its operability. In short, given the particular issues and circumstances of this case, the government's retention of the original computer even after the search was completed was warranted.⁶

In sum, the Court concludes that there is no basis to suppress the evidence recovered from defendant's laptop pursuant to the search warrant. Accordingly, defendant's motion to suppress that evidence is denied.

⁵ In fact, a substantial authentication issue arose during the trial in connection with a recording on defendant Kenner's seized cell phone, and counsel for defendant Constantine considered having an expert inspect the original recording on the phone.

⁶ Additionally, the government asserts that the device is subject to forfeiture, because it was purchased with the proceeds of the alleged fraud. (See Government's May 31, 2015 Letter, ECF No. 259.) The Court concludes that this is an additional basis for the continued retention of the device.

III. MOTION TO SUPPRESS EVIDENCE SEIZED FROM DEFENDANT'S CELLULAR PHONE

Although the defendant's motion focuses on the retention of his laptop, the motion also seeks the suppression of any evidence seized from the defendant's iPhone on the same grounds. As an initial matter, it is unclear from the defendant's motion what evidence Kenner seeks to suppress that was seized from his iPhone. The Court is only aware of one item of evidence seized from the phone that the government sought to introduce at trial: an audio recording of a conversation between the defendant and his co-defendant, Tommy Constantine. The government was clearly permitted to retain the iPhone as evidence, because Kenner's co-defendant, Tommy Constantine, has repeatedly challenged the authenticity of the audio recording. In fact, in his pre-trial motions, Mr. Constantine has argued that the recording was altered. (Motion to Suppress, ECF No. 157-14.) As noted *infra*, this authentication issue also arose during the trial. In order to respond to these concerns, the government had a clear need to retain the original iPhone, which was used to make the recording and contained the audio file that was seized by the government.

Notably, the authenticity challenge to the audio recording presents a categorically different authentication problem than the issue presented in *Ganias*. In *Ganias*, the government's authentication concern was whether the mirror image hard drive was an accurate copy of the original—with respect to both the metadata on the computer and the documents contained on the hard drive. In other words, the government was concerned about proving that certain documents and data on the mirror image came from the original hard drive. The issue in this case is markedly different, because all parties agree that the recording came from

Kenner's iPhone; the question here is whether the recording itself was purposefully altered and edited. That specific question requires the government to retain the original device, in order to offer evidence of the recording's origin and the manner in which it was created. For example, if the original file is still located on the phone, the government could offer evidence to show how a recording made on an iPhone can or cannot be edited. Thus, the original phone—and not merely the audio recording—has independent evidentiary value.


Attorneys. Defendant Phillip Kenner is represented by Richard Haley, Haley, Weinblatt & Calcagni, LLP, 1601 Veterans Memorial Highway, Suite 425, Islandia, New York 11749.

For these reasons, the Court concludes that the government's retention of the iPhone was reasonable, and suppression is, therefore, unwarranted.

IV. CONCLUSION

For the foregoing reasons, the defendant's motion to suppress is denied.

SO ORDERED.

 JOSEPH F. BIANCO
United States District Judge

Dated: August 28, 2015
Central Islip, NY

* * *

The United States is represented by Kelly T. Currie, Acting United States Attorney, Eastern District of New York, 271 Cadman Plaza East, Brooklyn, New York 11201, by Saritha Komatireddy and James Miskiewicz, Assistant United States